Chairman Peters Opening Statement As Prepared for Delivery
Full Committee Hearing: Cyber Regulatory Harmonization
June 5, 2024

The Committee will come to order.

Cybersecurity remains one of the greatest challenges facing our nation. As we have become more reliant on technology and digital infrastructure, the threat of cyberattacks has dramatically increased. Every day, our citizens, our critical infrastructure operators, and our federal, state, and local governments have to defend against hundreds of thousands of potential cyberattacks.

These come from criminals who take advantage of vulnerable people; foreign actors who threaten our critical infrastructure, and hackers who try to destabilize American businesses. Cyberattacks are more coordinated – and more dangerous – than ever.

In response to this threat, American regulators have begun to set new standards for cybersecurity and digital safety. They have moved quickly in that work. In the last four years alone, federal regulators have passed 48 rules on cybersecurity – more than 10 per year. And that doesn't include new policies at the state and local level.

This surge of regulations comes from a good place. It represents our government's response to a new and growing threat and has helped give American businesses some important guidance on how to keep safe from cyber threats.

The challenge is that even though all aspects of our society are vulnerable to cyberattacks – from electric grids to water systems to gas pipelines - no one is coordinating this effort. This is a patchwork of new guidelines set by separate agencies. Regulators are working to respond to the unique challenges their sectors face – and they are often not looking at the bigger picture of how all these rules interact. Without that higher level coordination, there is no way to ensure that these guidelines don't overlap, duplicate, or contradict each other.

The results are often confusing and inefficient. Businesses are scrambling to follow a web of new standards – ones that can change quickly with new technological innovations. Airlines have to adhere to three different regulators on cybersecurity. Railroads can have six. A bank could have *sixteen* different oversight bodies – all of whom are passing their own standards, expecting to be followed. This is not necessarily a case where more is better. We must be smart in these regulations to ensure the highest level of cybersecurity.

In short, businesses and their employees are spending too many resources trying to understand these new guidelines. Companies are taking their cybersecurity professionals off the line to fill out paperwork, leaving their defenses undermanned and vulnerable.

We need effective regulations on cybersecurity. But we need them to be efficient, adaptable, and coordinated across different agencies. Harmonizing these guidelines will make our government more efficient, help businesses compete on the global stage, and ensure that we're addressing cybersecurity threats in the most effective way. That is why I am working on legislation to

establish a Harmonization Committee at O-N-C-D that would require all agencies and regulators to come together, talk about cybersecurity regulations, and work on harmonization.

Passing legislation is the only solution. We have to bring independent agencies together and start harmonizing this effort. Only Congress has the power to do so. If we fail at that mission, we won't be able to build the most effective response to cyber threats.